They want to put me out of business. I could be murdered by hackers in the next couple of months.

They know I know their identities. I have 7,000 of them logged on my computer. They laugh at the FBI, the Secret Service, but they don't laugh at me. I was one of them.

'They live in a world in which they are gods. I force them to recognise themselves for what they are. I'm the one who rips off their masks.'

JOHN MAXFIELD, computer security consultant and former FBI informant

Burnt-out buildings rub shoulders with banks that have gone bust on Detroit's north side. Here, on forgotten avenues dotted with abandoned cars, sheets of plywood board up businesses that have packed up and left, in search of customers that have gone before them. Two motorcycle gangs, the Scorpions and the Forbidden Wheels, provide deafening tributes to horsepower for members of the nearby First Psychic Church of Brightmoor.

Even the quiet of tree-lined streets is punctuated by fire bombs and gunshots. Vacant flats have been converted to crack houses, drug dens for the severely addicted. In the local high school, as a means of reducing violence by confiscating weapons, students pass through metal detectors before entering the classroom.

Amidst this study in urban decay, John Maxfield operates out of an old distribution warehouse sandwiched between the faded storefronts of two beauty parlours. The harsh odours of permanents and hair colourants mix with the hot fat smells of a fried-chicken outlet located at the mouth of the alley that Maxfield drives down each day. Arriving at the guarded entrance of his headquarters, Maxfield parks his dented white Dodge van and dials a secret code on a telephone by a jailhouse door. He pushes two buttons in sequence and the barred door releases. With another formula of codes, Maxfield opens a thick, battleship-grey door made of steel. As it closes, it automatically locks behind him. In the dim light, shadows of machinery emerge in an ante-room the size of a small factory, leading to his office. Some of the hobbies Maxfield stores here have collected dust for decades. Over a thousand pieces of wood are assembled in a six-foot-long model of a street car that shares a table with dog-eared blueprints. An old-fashioned telephone booth from the 1940s, fully operational, is nestled in a corner.

A machinist's lathe occupies another. Thick snakes of bright telephone wire coil round milk crates, filled with electronic switches, resting on a cold, concrete floor.

Maxfield's office illustrates his early life's passion for telephones, computers and Star Trek. His desk resembles the bridge of the Starship Enterprise. A bank of six monitors, green, black and white, and amber-screened, form an L-shaped console. There is a field of buttons, switches and blinking lights surrounding telephones, intercoms, disc drives and recording equipment. A Tokyo subway map lies next to a button warning, 'My Laser is Set on Stun'. Resting above the console a model of the USS Enterprise scans the surroundings. A voice communication cabinet bears the sticker, Star Fleet Computer Division'. Nearby, an entire telephone exchange, suitable for a small town, hums and clicks. Maxfield built it when he was 18, from salvaged equipment that included parts from a Japanese PABX switchboard from Vlasic Foods Inc., a company famed for pickles.

Across the hall, a huge storage room is filled with computer and telephone equipment Maxfield has purchased from businesses upgrading their technology or going into liquidation. Nearbyis a collection of hacksaws, chisels and sledgehammers used to prise open the old computers. Maxfield, apart from living out the fantasy of a frustrated PC user, hacks away at them to retrieve valuable circuitry containing fragments of gold. When he has extracted enough, he takes the circuit board and chips to a smelter in Chicago.

Ribbons of connector cables drape over diodes, chips and wiring crammed on to steel shelves that take up an entire wall of Maxfield's storage room. A thick coat of dust shrouds a teletype machine from the 1930s. A collection of old black telephones stand silently to attention by a model train from the Mohawk Valley Electric Railway. Amidst all the machinery, dust and salvage, there is a sentimental reminder of what John Maxfield was up to when he was a kid. Alongside a crate filled with old headsets, sits the computer he built in 1953 out of an old pin-ball machine. He was 12 at the time.

A small room adjacent to Maxfield's console houses the heart of his operations. A bank of high-powered computers, 5½ feet tall and 4 feet wide, gently whir. For his own personal computer, Maxfield uses what amounts to an aging mainframe. A Hewlett Packard 2000 Access System flexes its strength with 99 megabytes, a 64K memory and, unlike an ordinary microprocessor's 8 megahertz, Maxfield's HP sports three disc drives, the size of small refrigerators, spin at 3,600 r.p.m. Maxfield keeps a humidifier next to the high-speed printer that is capable of printing 450 lines per minute. The steam keeps churning print-outs from jamming. Maxfield uses the energy of his computers to warm his office in winter. Apart from their central-heating value, the machines are worth about $300,000.

The only bugs in Maxfield's system appear to be the rubber centipede and cockroach he has glued to a printer. On another, a bright-orange furry doll of Garfield, the cartoon cat, poses with nonchalance while Captain Kirk, three gold stripes on the cuff of his mustard uniform, stares out from a poster. A life-size cardboard cut-out of Mr Spock lends a logical feel to the place. The word THINK looms out above the twenty-one switches on the HP 2000. Next to a disc drive a bumper sticker implores 'Beam Me Up Scotty - There's No Intelligent Life Here.'

When he was tested for intelligence, Maxfield discovered he had an 1Q of 179. Whether by choice or consequence, Maxfeld has always been somewhat of a loner. In high school, while everyone else was learning the Twist, he was building a telephone exchange. That sense of isolation still exists in Maxfeld's work. In a building without windows, Maxfield gets input from the outside world through a panel of blinking lights attached to a photocell and an anometer on the roof. Red indicates the weather outside his office is cold; yellow, stormy; green, warm; blue, fair.
On a 'green' morning in May, Maxfield wears his only uniform: a white short-sleeved shirt, two pens and black spectacle pouch in the pocket, a black leather belt, dark-blue trousers, black socks, and black leather utility shoes. Maxfield's black hair shines with grease and he wears black horn-rimmed spectacles. His mouth is framed by a thick moustache and goatee. The man rarely leaves his office and it shows: his skin has the pallor of a submariner. 'I'm your basic nerd,' he explains. 'I was always the runty one the kids picked on.'

The only child of two librarians, Maxfield grew up in Ann Arbor, Michigan. Each day after school, he used to visit the telephone exchange with the same devotion other kids had for baseball practice. When he was 9, Maxfield invented a crude switchboard. Three years later he built his first computer. It was when Maxfield's attention turned to telephones that he installed his own telephone exchange. One day he dialled up all of the circuits from Ann Arbor to Chelsea, Michigan, in tandem until all of the phone lines of the two towns were fully engaged. It took Maxfeld, then 15, all of ten minutes.

Soon afterwards, he began teaching his high-school classmates electronics. One day, Maxfield spotted an intriguing advertisement in the Saturday Evening Post. It amounted to a public-service announcement placed by the telephone company.

It proclaimed that operators could finally establish long-distance connections without having continuously to relay calls from one operator to the next. 'When they printed the ad,' recalls Maxfield, 'they also printed the musical notes representing the tones of the numbers.'

Using what was available to him, Maxfield held the mouthpiece of his telephone against the sounding board of his parents' piano and played the corresponding notes.
'I was able to connect my call, free of charge. You didn't need anything electronic.' Maxfield escaped being billed for his call because, 'They made the mistake of publishing, for all the world to see, exactly how the long-distance system worked,' he says. 'The engineer that designed the system warned them that, if people started using home-made tone generators, they could start making free calls.'

In 1961, using pieces from scrap bins and pointers from a Bell System technical journal, Maxfield invented one of the first 'blue boxes, a sort of push-button keypad connected to amplified tone-generating circuitry. With it he was able to make illegal, long-distance calls. For Maxfield, it amounted to a portable piano.
He became what's known in the trade as a 'phone phreak'.

'Phreak' was coined in the early 19705 as the title given to someone who is able to make free but illegal long-distance telephone calls. Maxfield says his brief phreaking career came to an abrupt end when a man from Michigan Bell's special audit department stopped by his house for 'a chat about the facts of life and the phone company'.
Curious company executives who had never seen anything like Maxfield's invention decided to make a deal with him. They would not press charges as long as Maxfield co-operated. 'Theygave me three conditions. One: Don't do it again. Two: Tell us how you did it. Three: Don't tell anyone else.'

Besides inventing a blue box, Maxfield simultaneously created the first black box that permitted a user to receive incoming calls free of charge to the dialer. Because the caller could not be disconnected until the receiver of the call hung up, the black box proved very useful as a trap-and-trace device for police dealing with bomb threats. In 1964, at the age of 23, Maxfield received a patent for his black box.

He applied his knowledge of electronics to a career that would keep him in constant contact with the machines he had mastered. He began installing his own telephone systems and servicing facsimile and teletype machines. Maxfield travelled a daily 200-mile circuit around Detroit, mending and maintaining machines that sent information and images from satellites to television screens, from offices to overseas branches. During the day he carried a tool box, and at

night he played with his computer.
In 1976, Maxfield joined a new club for computer enthusiasts.

Instead of meeting in a coffee shop, the club met electronically, accessing time on a local school-district's computer, provided for their use, after hours. The club created one of the first electronic bulletin boards systems (BBS). A BBS is much like the notice board found at a local shop - a place where messages are displayed. Maxfield was elected treasurer of the club and supervised the bulletin board and the system's software, most of which was written by him and his friends.

As the years went by, more bulletin boards were set up by computer users. All that was required to operate a BBS was a computer, some software and a modem (a device enabling computers to receive and transmit information via telephone lines). Some of the bulletin boards were exclusive, requiring users to enter secret passwords before gaining access. Sometimes prospective members of a BBS had to pay an entrance fee in the form of a software package. In turn, the new member might receive five software packages from existing members. Almost without exception, all of the proprietary software exchanged was illegally copied, or pirated. Soon bulletin boards became the central source of software piracy in America, Feeling the pinch of lost sales, software publishing companies sought legal remedies to the pirate problem. Because the stolen software was being transmitted through telephone lines (via a modem, connected to a computer), the crimes being committed were copyright infringement and computer fraud, then known technically as wire fraud. At the time, these cases were handled by the Federal Bureau of Investigation (FBI). In years to come, computer fraud and abuse would fall under the jurisdiction of the Secret Service following the passage of the US Computer Crime Bill in 1984.

In August of 1982, the FBI began making enquiries at computer stores in the Detroit area. One day an agent approached the president of Maxfield's computer club, explaining that he was chasing down leads in a software piracy case.

The president of the club told Maxfield about the visit. 'They are looking in the wrong place,' said Maxfield.

'At that time,' he says, 'we were getting advertisements for pirated software on our BBS, but it was of no interest because we wrote our own.'

His curiosity piqued by the agent's visit, Maxfield called up local bulletin boards and ran print-outs of their messages. Users boasted about computer systems they had gained access to and Maxfield documented some illegal software swaps.

On an early September morning, he loaded up his van with tools and drove to the Ann Arbor weather bureau. Finished with his monthly equipment check, Maxfield wandered down the hall and entered the regional office of the FBI. He introduced himself to the agent who had approached the president of the computer club and said, 'Ive got information on the pirates you're looking for.' Maxfield pulled out the sheaf of computer print-outs detailing illegal software transactions. The man wanted to know how Maxfield had obtained such incriminating evidence. Maxfield explained that by hooking up his computer to a modem and using some software, he was able to dial up local bulletin boards and retrieve information for the price of a telephone call. 'Wait a minute. Stop right there,' said the agent. 'What's a modem?'

Maxfield suddenly looked around the room and noticed there was not a single computer in the office. 'How do you keep track of criminals without computers?' he asked. The agent pointed to a card file. Maxfield started from scratch, explaining what he knew about bulletin boards, modems and software piracy.

''At least half of all computer bulletin boards exist solely for the purpose of piracy. There are hundreds of software pirates operating on the boards, each one trying to out-do the other and be first with the latest version. Do you know what the street life of an average video game is?' he asked the agent. 'Well, it's negative two weeks. The pirates have it two weeks before it hits the stores because they get it right from the wholesalers or from the publishing house directly.

'I've seen stuff that wasn't even finished product, just partially completed games, that the pirates had three months before the stores had it. The bottom line is that many of the computer criminals start out as software pirates. The hacker underground is their introduction to the world of crime.' Maxfield didn't know if the agent understood a thing he had said. The man just nodded, expressionless.

Two weeks later, a young man who looked like a university student knocked on Maxfield's door. He was an FBI agent from the Detroit office, in charge of the software piracy case.
Maxfield explained how the bulletin boards were used by pirates to trade illegal software and showed him the BBS

print-outs. 'Going back to my experience as a phone phreak, in the r9sos and I96os, I knew what could happen,' recalls Maxfield. 'You could invade military and private data bases.' Maxfield began at the beginning, telling the FBI agent about Cap'n Crunch, a phone phreak named after the breakfast cereal that contained the prize of a little whistle. The whistle identically mimicked the radio frequency tone used to tap into telephone lines. Cap'n Crunch used whistles illegally to wiretap and wound up serving jail time as a result. Then there was the Roscoe gang in Los Angeles, the first reported group of computer hackers to hit the scene. 'I was shocked the FBI didn't know anything about computers and their potential for crime,' recalls Maxfield.

It was a detailed meeting with Maxfield decoding computer jargon to an agent trying to refrain from legalese. Maxfield had access to this foreign world of computer hackers, and he wanted to help. After all, he was already providing evidence.

The agent made a proposition that would change Maxfield's life: 'Could you be an informant for us?' Maxfield agreed, on condition that he would not be billed for his long-distance calls to the bulletin boards.

After the agent had gone, Maxfield remembered the promise he had made to the telephone company when they took his blue box away. He had kept the three conditions for over twenty years; now he was being given permission to break them. 'The FBI gave me an excuse to recreate what I had as a boy,' he says.

I was given a licence to phreak and hack. To do what I always wanted to do but was afraid to. Suddenly I was able to return to 1961 and pick up where I left off.' Maxwell adds, 'I was an amateur. I had no legal or law enforcement background. In the beginning, it was the blind leading the blind.' Within a matter of weeks, Maxfield was introduced to a vast society of hackers, each of whom had a different mission, achievable with the help of computer technology. Some were harmless thrill seekers who broke into complicated systems for the sake of penetrating a new sphere of technology. Others cared not so much about the artistry of cracking codes as creating chaos once on the inside. The ramifications were serious enough to draw the attention of federal agents. Their fear was that the power of computer technology had fallen into dangerous hands.

Maxfield began to see the evidence of criminal and malicious hacking: espionage, extortion, theft and credit-card fraud. He began to monitor the hackers and recorded their recipes for explosives and poisons. 'Logic bombs', 'viruses', 'worms and 'trojan horses' were the heavy artillery of the computer anarchists under his surveillance. The hackers, with names like Brain Tumour, Dr Death and Axe Murderer, had crossed the divide of fun and games and had entered what Maxfield termed the dark side of the force'. For the next eighteen months, Maxfield would enter their world and, ultimately, fight for his own survival.

In the early days of computers, a hacker was a pioneer - someone intimately involved with the internal makings of a computer; someone who attempted, like the captain of the Starship Enterprise, to 'boldly go where no man had gone before. The term hacker' was originally used to describe Massachusetts Institute of Technology (MIT) students in the 196o who became obsessed with the computer. Their aim was to make the computer a beneficial tool for society. Later, 'hacker' applied to a computer user whose path of discovery involved trespassing on unguarded systems. In the traditional sense of the word, Maxfield is a hacker, whereas the new breed of hackers he was about to chase were guided, in his opinion, by two fundamental principles: that knowledge is power, and that there should be unrestricted access to computers, particularly those with sensitive data bases.

The sense of harmless exploration and invention embodied by early hackers gradually devolved into exploitation of data communication facilities by the new generation of whiz-kids who cared little about how a computer actually worked. The electronic machine was no longer a 'learning tool. It had become a vehicle for criminal activity

The criminals were not easy to catch. Their computers gave them the chance to commit a kind of ephemeral larceny: silent, undetected, rarely punished. It was a safe form of robbery and extortion with no trace of fingerprints and, without ever encountering the victim, no guilt. 'Hacking is a completely impersonal, dehumanised crime,' says Maxfield. None of them would dream of taking a knife or a gun and mugging someone on the street. The hacker doesn't know his victim and the victim never knows the hacker. There is never any physical risk involved. They are introverted thrill seekers.' It's mob psychology but with an electronic twist.

Maxfield began to notice a form of electronic schizophrenia on bulletin boards. 'Face to face, the hacker is perfectly nice, well mannered, well behaved and polite. Someone who has never been in trouble, someone who is introverted. But when they get behind the keyboard, they unleash their imaginations and hidden personalities and they turn into Genghis Khan or Adolf Hitler. A 12-year-old I knew called himself Napoleon Bonaparte.' On a BBS he noticed a certain equalisation taking place.

There are no class distinctions,' says Maxfield. "A hacker becomes iust a voice on the phone or just a message on a bulletin board. It's like the Walter Mitty syndrome carried to the ultimate extreme. With a computer, hackers can carry out their wildest fantasies. And there is no one supervising them.

It's the alternative to a street gang. The hacker is a street-corner hood, except today the meeting place is a bulletin board?' Operating with an electronic anonymity, hackers key into boards named 'Sanctuary, 'Futureworld', 'Darkside', 'Death Trap' or 'Speed Demon Elite'. A BBS is an equaliser, upon which the physical appearance of the hacker is never called into play. Instead, what counts is the level of daring he performs in 'cracking' into sensitive computer systems. His hacking skills are displayed when he posts on the BBS the secret passwords to the restricted data base he has broken into.

The British science-fiction writer Arthur C. Clarke expressed that high technology is indistinguishable from magic. Maxfield believes hackers understand the power of magic. "They live in a fantasy world where a computer password is the equivalent of a magical incantation, like an old-fashioned wizard might use,' says Maxfield.

Passwords allowed computer users to go certainly where no teenager had gone before. Demographic studies conducted on known hackers reveal that they are for the most part teenage boys, although ro-year-olds, college professors and a few girls have also become hacker gang members. An FBI agent described them as 'bright, affluent and bored' Being a hacker became the perfect remedy for adolescent ennui. What could be more exciting than marauding sophisticated computer systems with an alias such as the Stainless Steel Rat, King Blotto, Satan's Stronghold or Black Knight - especially when your voice has not yet broken?

Maxfield's initial brief was to identify hackers who traded illegally copied software. He would gain access to a bulletin board and methodically write down their details on recipe cards.
'Then I called a BBS in New York City, where the real hackers hung out,' says Maxfield. He was in for a surprise. I have a friend who is installing a new computer at the Pentagon,' read one. 'He's giving us the password next week.'

'This was thirty days after I started working for the FBI,' recalls Maxfield. 'So, suddenly, we went from little kids passing around illicit software to someone who was now threatening our defence policy. We were playing hardball. That's when I decided it had to be more than a part-time activity. I felt a sense of obligation. What really concerned me was this lack of understanding of what a computer could do,' says Maxfield.

"When you're talking about a true hacker, you are talking about an explorer. The problem is that in the course of your explorations you find out not only how things work but how things are flawed. You think about how to exploit the flaw, to make things work to your benefit and, at that point, you've
crossed into that grey area. If you continue further you're into the criminal area. You're into what I call the "Dark Side of the Force". The dividing line is not very clear,' says Maxfield, but I've always known where the line was. I always knew when I crossed the line and I think the hackers know, but they don't care. If something happens, if they think someone is on their trail, all they have to do is hang up the phone, disconnect the line and they're gone. In a sense, they are untraceable. They are invulnerable to any detection. I was the only person who volunteered to help. I became the Lone Ranger out there.' Following the Pentagon disclosure, Maxfield knew he could no longer remain on the sidelines. 'I've got to join this underground,' he told himself. The question was, how?

While gathering intelligence, Maxfield discovered a bulletin board featuring a section for the exchange of stolen long-distance dialling codes and information on hacking. He made friends with the BBS operator to find out what was going on. After several telephone conversations and bulletin-board messages, the BBS operator said, 'Look, you know much more about hacking and phreaking than I do. Why don't you run the hacking and phreaking section of the bulletin board?' Maxfield accepted and soon the FBI gained an insider's look into the computer underground. 'We were running it as a sting,' says Maxfield, 'unknown even to the bulletin-board operator himself. He developed a handle and called himself Cable Pair, the first phone phreak, and then devised an enticing gimmick for his prey. He set up a 'training school' for hackers on the newly created 'sting board'.

'I was going to teach them the basics of how the telephone system operated. I wasn't going to teach them anything that wasn't already in a technical manual. But I had to make it sound like they were going to learn something really super nasty. I had never had any training as an actor, never had any thoughts of doing anything like that and, suddenly, I was involved in acting, role playing. I did what I thought I should do and it worked.' Within seventy-two hours, Cable Pair received calls from the Glitch, the Sprinter and the Wizard, and two dozen more hackers from around the US.

'The objective was to penetrate through the alias to the real person and in order to do that all I needed was their home

phone number,' says Maxfield. 'For instance, if the Mad Hacker was posting Sprint (an American-based long-distance telephone company) codes, we had all we needed to find out his real identity. We would make friends with him somehow through introductory messages. He would log on the bulletin board a day or so later and read my message that I had sent privately to him and he would call my phone number, using one of the stolen Sprint codes. We had a back trace if we needed, but, more importantly, I would be talking to him one-on-one over the phone, on a little more personal basis.'

During the telephone conversation Maxfield could find out what the Mad Hacker was doing, how he was doing it, what kind of equipment he had, what sort of computer, what other bulletin boards he was calling. Maxfield would say, 'Hey, I gotta go, it's dinner-time. Can I call you back later? What's your number?' And the Mad Hacker would unwittingly become an entry in Maxfield's FBI file.

Beginning in September 1982, Maxfield gathered evidence from hackers eager to learn about phreaking. Hackers soon discovered that 'BBSing', while fun and absorbing, can be terribly expensive, carrying the equivalent costs of marathon long-distance calls. One hacker spent sixteen hours a day on the telephone lines, accessing BBSs all over the world. Using stolen long-distance codes he ran up a bill of $400,000 before being caught. The simple solution for hackers was to learn how to make free telephone calls. Maxfield's 'training school' drew eager hackers ready to learn the fine art of blue boxing and phreaking. While he spun together vague abstracts on telecommunications, Maxfield gleaned valuable tricks of the hacker trade.Maxfield monitored numerous boards, each of which had its ownraison d'être. He noticed that on some, for example, detailed tutorials on various aspects of hacking appeared, accompanied by access codes to restricted data bases. It became clear to Maxfield that he had entered a world in which there was an orderly progression of hacking feats that lead to a lexicon of computer crime.
As Maxfield scanned the boards he began to establish a rapport with his targets. Through their messages, he learned that hackers, armed with computers and modems, had begun trespassing into private computer systems, including those belonging to corporations, foundations, universities and banks.

Hacker gangs began to go 'carding, using valid credit-card numbers obtained from discarded carbons, accounts posted at video rental stores, or even by hacking credit-bureau computers.
'Trashing' was another trick. Hackers sifted through trash to find thrown away computer passwords and code words and confidential company phone directories. Corporate trash,
Maxfield learned, is a hacker's treasure chest.

One day, Maxfield found a four-part tutorial on credit-card fraud posted on an exclusive east coast BBS dedicated to advanced hacking. Its creator posted the warning, You MUST have a fluent tongue and a semi-deep voice (skip this part if your voice is still cracking - refer back when you get a real one).' Maxfield was having a field-day. When he started, he counted between 400 and goo hackers on the boards. Within two years, their numbers would increase by a factor of ten. The hackers form little cliques and gangs, so I went after the top ones. I didn't bother with the little kids who didn't know anything because they weren't really a threat,' says Maxfield. 'In the process, I had to talk to them all. By setting up the sting operation, they came to me. I had to do a lot of analysis and decide who was who and who was the bad guy and who was the casual kid who liked some software now and then and didn't pay for his phone calls. No one was going to prosecute that person, but the person who was deleting files in some government system - he was a threat and he had to be identified and dealt with.' At the beginning, Maxfield says, 'We had no intention of arresting anybody. We were strictly doing intelligence gathering.

The FBI had really no background to the nature and extent of the electronic underground. So we spent probably the first six months just gathering information.'
Soon after Maxfield began working undercover, in November 1982, one of the bulletin-board operators decided to have a piracy party and invited all of the users to his house for a huge software swap. Maxfield, who had become a member of the bulletin board, was invited. He left a message with the system operator (sysop) asking if he could bring a friend. The sysop said, 'Oh sure, the more the merrier.'

Maxfield's friend was an FBI agent. Both of them were operating undercover. They parked a quarter of a mile away and set up a camera on a tripod in the parking lot of a nearby high school. With a powerful telephoto lens they began taking photographs of teenage hackers emerging from their parents' cars, lugging their computers into the sysop's house.
'It was just like on TV,' recalls Maxfeld. 'You're sitting there with binoculars watching the bad guys drive up in their cars.

You take a picture of the licence plate and call it in on the radio to find out who the car belongs to and then, as they get out the car, you take their picture.' When Maxfield and the agent finally arrived at the party they were led to a recreation room. 'There must have been about twenty computers and forty people. The room was jammed. Everybody was copying software like crazy. In that afternoon, over $100,000 worth of illegal software changed hands.'

The BBS computer and its modem were surrounded in a corner by a group of hackers trying to break into a university's mainframe. The FBI agent, who looked like he was a student dressed in a T-shirt and jeans, walked over and made friends with a college professor who had brought some equipment from his university to the copy party. The professor ran off duplicates of copyright software and gave it to the FBI agent.

'Meanwhile,' says Maxfield, 'I spoke with some pirates and I mentioned that I was one of the original inventors of the blue box. And this guy jumps up and announces it to the whole room. All of these hackers converged on me. Well, at about that moment, the doorbell rang and one of the hackers said,

"Oh my God, I hope that's not the FBI!" I looked over at the agent and I couldn't keep a straight face.'

The party was useful. It provided Maxfield with introductions to hackers, while his notoriety as Cable Pair spread. After the new year he began noticing an influx of names appearing on the bulletin boards. Teenagers who had received computers for Christmas began testing their data-communication skills. The Hacker, a 14 year old from Detroit, stood above the rest. The Hacker's parents had given him a modem for Christmas, and with it he and his $250 Atari 400 travelled through computer systems all over the US. The Hacker became co-system operator of a BBS called the Secret Service. It was the creation of a 12-year-old hacker in Los Angeles by the name of Megabyte.

The Secret Service BBS had a hidden section requiring a special access code.

BBS access numbers are as closely guarded as secret formulas.

Some are posted on underground boards, but to gain access to their hidden sections is extremely difficult. Computers at the Department of Defense, like hundreds of businesses, give an indication when you've reached them. But with some BBSs one is required to know a password in order just to find out what BBS is on the other end of the modem. Once engaged with a system, a user is required to give his real name, phone number, address, occupation and interests. The sysop will then call and give a secondary password, provided the caller has passed scrutiny.
Maxfield monitored Megabyte and the Hacker, carefully making notes of the stolen long-distance carrier codes hidden in the secret section of their BBS He fed the information to the FBI, and to MCI and US Sprint, the long-distance telephone companies whose codes had been stolen and posted.

On a Friday morning in May 1983, investigators from the Los Angeles Police Department, armed with a search-warrant and joined by representatives from Pacific Telephone (the local phone company) and Sprint, walked into Megabyte's house and 'cleaned his bedroom for him', says Maxfield. Megabyte was charged with 146 counts of wire fraud and placed on probation.
Maxfield, meanwhile, had become good friends with the Hacker, who he also knew as Eric Stajda, freshman at DeLaSalle Collegiate High School in Detroit. 'He seemed to be the one to watch,' says Maxfield. 'He had been talking about wanting to be on defence systems. He was special,' says Maxfield. 'He was on the boards all of the time. He was on dozens of them. Once he learned how to phone phreak, it was a full-time occupation.' Maxfield, who had met Eric through the Secret Service BBS, called him the day after Megabyte's bust.

'Eric, aren't you afraid?' asked Maxfield.

'I'm not worried,' he said. 'I live 2,000 miles away. I'll just change my handle.'

Overnight, the Hacker became the Wizard of Arpanet and a founding member (and eventual leader) of the Inner Circle gang. The Inner Circle communicated through the Security Land BBS, an élite, Beverly Hills-based bulletin board created by a hacker called Napoleon Bonaparte. The Wizard's new title reflected Stajda's dedication to cracking defence systems within the Advance Research Projects Agency Network, or Arpanet, for short.

Regarded as one of the most vital data networks in America, Arpanet links the Pentagon with 30o mainframe computers and 50,000 users at universities, defence contractors, the Pentagon and other Department of Defense locations for the exchange of classified and non-classified information. 'It might be nothing more than annual budget information,' says Maxfield, or it could be very sensitive and classified, like the results of some kind of missile guidance-system development project.'

Normally if a hacker wanted to break into Arpanet, he would find out a password. Unless they are very facile, you don't guess passwords. You steal them. 'So what would happen is this,' explains Maxfield. 'You might have a hacker who is an airman in the Air Force, or he has a friend in the military or a government official or someone who has access to

where the computers are and, by one means or another, he obtains a password.'

The Wizard continued making inroads into the Arpanet's system. One day, he managed to break into the Pentagon. 'The Wizard had found a way to get a dial tone from inside the Pentagon,' explains Maxfield. 'He had heard from somebody that there was an 800 number you could call and if you knew what to do you, you would get a Pentagon dial tone. The number belonged to the Defense Department,' says Maxfield.

At that point you could dial anywhere the Pentagon could dial, at the Pentagon's expense. These included all the defence circuits on the Pentagon's private network, just like in the movie War Games. You could access Department of Defense computers, anything, provided you knew the phone numbers and the passwords.
'Well, my phone rang one day and it was the Wizard, and he says, "Cable Pair, listen to this!" The next thing I know, he three-way connects me with a general in the Pentagon and he's talking to the general... 'The Wizard pretended he was another general somewhere. Of course, because he had a very young sounding voice, the conversation degenerated very rapidly. The name he chose was totally bogus and I kept wanting to break in on the conversation and say, "Eric, hang up!" I couldn't even hang up because then it would be obvious that somebody else was on the line, so I just had to hold the phone and, finally, the general hung up his phone and that was the end of the call.'

With the Wizard as their founding leader, the Inner Circle gang began targeting other defence areas. One night they tried to order a red alert at NORAD, the North American Air Defense Command headquarters. There was a hacker who was the son of a British diplomat and he had access to various secret codes. For example, all high-ranking members of government are assigned a code-name. At the time, George Bush, Vice-President of the United States, was known as Timber Wolf. So, if you called up a certain unlisted telephone number that the hackers had found out, which rang at the White House switchboard, and said, "I want to speak to Timber Wolf," you were connected to George Bush, no questions asked, no matter where he was.

'So they were calling up NORAD and ordering Red Alerts:

"This is Timber Wolf, I've got a code three . . ." They never really got anywhere with it, but the point was, it got everybody in an uproar. Needless to say, the Secret Service was not pleased, nor was the State Department when they learned who was the source of the codes. All of the codes had to be changed.

The diplomat's son, who had diplomatic immunity, had to be persuaded not to do this any more,' says Maxfield.

'They also found a way to bill telephone conference calls, 59-way conference calls, to the White House switchboard. So they were giving President Reagan big phone bills for their phone-phreak conferences. It was just an incredible, wide-open scene. The Inner Circle was already doing the stuff that was in War Games before the movie came out. Afterwards, there was a tremendous explosion of activity.'

War Games, the movie about two teenage hackers who penetrate government defence computers and nearly start a nuclear war, produced an eager new crop of hackers. For the normally introverted teens, their technical prowess could be measured by a kind of modem machismo. At the time, Donn Parker, a computer and data security consultant at SRI International, a California-based non-profit research institute, commented, 'The malicious hacker problem is continuing to increase drastically and is getting far more serious. The lowering costs of equipment, the attraction for new kids coming into it as a rite of passage, points to an increasing vulnerability of American business to the hacker problem.' Parker's expertise ironically landed him the job of technical consultation to War Games.

By 1983, within months of the movie's release, Infocorp, a marketing research concern in Cupertino, California, reported that there were 600,000 computers at use in homes in the United States, a six-fold increase since 198o. Infocorp's president estimated that 120,000 to 180,000 of the computers were equipped with modems, the required instrument hackers use to gain access to bulletin boards and other computers.

Meanwhile, in his undercover role, Cable Pair had become an adviser to the Inner Circle, and maintained a number two position on their secret bulletin board. What the hackers didn't know was that with every encounter they had with him he gathered evidence to bust them. He monitored their calls with dial number recorders, so that he could determine where they were calling and what systems they were breaking into. Maxfield even got to know them personally, inviting hackers to his office at the height of the post- War Games frenzy. Kids travelled over 600 miles, from as far away as Washington, DC, to come and meet the veteran hacker and phone phreak, and to play with his equipment.

Most of the Inner Circle turned up: the Stainless Steel Rat, PBX Super Switch, Myth, System Lord, Mr Binary, the Rodent and, of course, their leader, the Wizard of Arpanet. Maxfield told them that he worked as a telephone-equipment

repair-man.

A couple of weeks after the get-together, Maxfield examined the messages on the Inner Circle's BBS and sensed a growing hostility between the Wizard of Arpanet and Mandrake the Magician, a hacker in New York. By now, the Pentagon trick was old hat. The Inner Circle had moved into the major leagues.
A San Diego Inner Circle member, known as the Cracker, discovered the access code to Telemail, a network service operated by the GTE Telenet Communications Corporation in Vienna, Virginia. Companies subscribing to Telemail paid. besides the price of a phone call, a minimum monthly fee of $500, and S14 an hour for use during business hours. The Telemail network links more than 1,200 commercial computers, including firms on the Fortune 5oo list of the biggest American industrial companies. It also has a fair share of government
accounts.

Mandrake the Magician, like the Wizard of Arpanet, was an Inner Circle system operator. In the manner of victors dividing up spoils, they divided Telemail's major accounts between them. One day, the Wizard was in a bad mood.

He called up Mandrake's mother in Scarsdale, New York and swore at her. Then he superimposed his user ID over Mandrake's and took the Magician's accounts, including the one belonging to the National Aeronautics and Space Administration (NASA). The Wizard left electronic cartoons and 'Kilroy was here messages for Mandrake and NASA agency employees to find.
Mandrake guessed the Wizard's password and proceeded to delete the Wizard's accounts (including NASA's), instantly destroying all of the electronic mail messages they held.
Incensed, the Wizard retaliated by wiping out Mandrake's Coca-Cola account. They waged their battle throughout the month of May 1983. Companies lost mail, had it rifled through or received shocking messages. One of the hackers' gimmicks provided cheap entertainment. They would send insulting messages signed by one executive to another and immediately fire offensive replies to the supposed originator.

Telemail had four different groups invading it. Besides the Inner Circle, there were the friends of the Inner Circle, Phalse (Phreakers, Hackers and Laundromat Service Employees) and random system abusers.

By June, Maxfield had identified the hackers. At that point, Cable Pair was asked if he wanted a Telemail account to play with. 'The Wizard,' he says, 'offered me a piece of NASA.' In the early part of the summer of 1983, according to Maxfield, GTE Telemail called up the FBI and told them someone had just destroyed their system. The FBI rang Maxfield.
They said, "Who's hacking Telemail?" I said, "Well, it's the Wizard and it's Mandrake the Magician and this guy and that guy." I gave them about twelve names. And so then they set up the trap-and-trace, and dial number recorders.'

In the end, the intruders had caused so much turmoil among the users of the Telemail network that the Telenet Corporation had to shut down the service. Hackers had changed the passwords of paying subscribers so they were unable to leave or collect messages. They found other ways of blocking subscribers from using the service and deleted information from corporate accounts. Investigators estimated the company suffered approximately $500,000 in lost time and repairs.

In mid October 1983, the FBI conducted simultaneous raids on the Telemail hackers. They hit the Wizard's home in Detroit, Napoleon Bonaparte's in Beverly Hills and issued search-warrants on hacker homes in Tucson, Arizona; Oklahoma City; New York City and upstate New York; and San Diego.

In all, computer equipment was seized from fifteen youths from coast to coast.

The Wizard of Arpanet became a minor celebrity. He even boasted, 'Hackers from all around the country were calling up and comparing the number of FBI agents who raided them. I had about nine,' said the Wizard. One guy in California only had three.'

Ultimately, the Cracker in San Diego and three other adults plead guilty to violation of Federal felony wire-fraud statutes, while six others would plead guilty to various misdemeanour charges. The juveniles, such as the Wizard, were not charged with crimes since computer intrusion was not yet regarded as a crime.

When he was busted, Napoleon Bonaparte (Bryan Green, a 17 year old at Beverly Hills High School) did not name names but said he knew of someone who had been 'bragging abour deleting mass quantities of data'.

'It was intentional,' said Napoleon Bonaparte. 'It's not like he slipped and fell on his keyboard and, the next thing he

knew, NASA was gone.'

A spokesman for NASA said that since the break-ins, the system has been changed completely, including the passwords.

He told the New York Times, 'It's much more complicated to get into the system.' (In September 1987, a group of West German hackers, belonging to the Chaos computer club, broke into the international computer network of NASA and rummaged freely through the data for at least three months before they were discovered.)

Maxfield's work continued. A hacker called the Iceman, leader of the Black Triangle, supplied a tutorial on conducting credit-card fraud on the World of Cryton BBS. Eventually, six high-school students purchased' thousands of dollars worth of computer-related equipment which was sent to a mailbox rental service in Waukesha, Wisconsin. The Secret Service, having been informed by Maxfield of the group, installed a video camera to monitor pick-ups from the box.

Maxfield had learned about the case through scanning the bulletin boards and forwarded information to the police. 'I've reported crimes to victims who didn't even know about it,' he says. Normally, a victim, having seen unaccounted charges on his credit card or telephone bill, files a complaint with a law-enforcement authority or contacts Maxfield through his company, Boardscan. If the victim is a computer operator, Maxfield analyses what data has been changed or destroyed and if the hackers left anything in the way of electronic fingerprints.
He writes everything down in an activity log.

My role is to identify the perpetrator. Once the suspect is identified, we obtain a court order to put a dial number recorder on the suspect's telephone,' says Maxfield. 'It's similar to a house being robbed ... you interview all of the neighbours.' Only in this case, the 'neighbours' are hackers signing on to the BBSs.

Maxfield has a network of twenty-five well-placed informants who make enquiries for him on BBSs all over the world. He is as tireless as his targets, who log on at all hours. 'It's a giant Dungeons and Dragon's game,' he says, referring to the addictive computer fantasy. 'If I can't catch hackers, I get really frustrated. I kill monsters or Klingons.'
Once the suspect is identified and Maxfield has sufficient evidence, a 24-hour search-warrant is issued. 'We hope to catch him in the act by monitoring his calls to the victim,' he says. The hacker is not arrested at the search-warrant stage, but the police obtain his logs, diaries, address books, long-distance codes and his computer. The next step is the analysis stage where Maxfield or police computer experts decode the evidence.

'Any good cop knows his local crooks like he knows his brothers,' says Maxfield. 'I know the hackers in the same way.

I read their messages and I probably know them better than their parents, yet I don't know what they look like.' Soon after his undercover work began, Maxfield noticed some new twists in the hacking game. The anonymous marauding instincts of criminal hackers gave rise to even greater thrills than simply cash rewards. A sense of anarchy prevailed. On a bulletin board in Phoenix, Arizona, hackers posted a recipe for thermite, an explosive chemical compound. Imahacker in Detroit posted recipes for pipebombs and poisons. 'Make sure you wear gloves,' he advised. Death can occur within sixty seconds of contact. You could get sick just touching this stuff. So be very, very careful.'

"Now this was a 14-year-old boy,' says Maxfield. 'An all As student in school, he had never been in trouble before in his life.'

On a board Maxfield monitored, called Black September, formulas for nitro-glycerine and plastic explosives shared the same data base as files on the Russian Embassy. Information on wire tapping and bugging was also available. The Black September gang: Brain Tumour, Surf Monster, Mr Mastodon, Dial Tone, the Rogue and Lord Shadow, created a step-by-step log-on procedure for breaking into TRW to attain credit histories. This BBS became one of the many which featured the credit histories of Ronald Reagan, Colonel Oliver North and Admiral Poindexter.
Hackers flexed their muscles in other ways. Extortion became commonplace. 'Hackers would obtain all the passwords to a computer system, and maintain complete control of the computer by remote,' says Maxfield. 'They would threaten to shut down an entire operation if ransom money was not paid or they would simply demand a free account on a machine and say, "Or else I'm going to destroy every other operating account."

More alarming were disgruntled data-processing employees who began posting anonymous messages on BBSs, requesting hackers to plant logic bombs, worms and viruses into their company's operating systems. A logic bomb is a programming code embedded into the system that usually instructs a computer to perform acts that can be both damaging and dangerous. A fired employee may have a hacker insert a logic bomb to modify the payroll system so that when his name is deleted, it will delete all other employees from the system. Worms, on the other hand, unobtrusively

absorb the memory of a computer.

Virus programs instruct the host machine to summon stored files and copies itself on to the files. The computer's memory soon becomes a mass of confusion.

There were times when the requests from angry employees were daunting. Mr Slippery, 12, never considered his hacking to be that special until one day he received a mysterious call from a stranger. The man offered Mr Slippery money to destroy a bank's records. 'At that point in time, I realised that it would be an incredible way to launder money. If I was real smart I would move out of the whole thing, because that was an obvious indication of organised crime to me.' Mr Slippery turned him down.

At the height of the hacking fervour that followed the release of War Games, Geoffrey Goodfellow, a reformed hacker working at the SRI research institute in California, said, 'If companies try to thwart the attacks on their mainframes by plugging the holes in their security armour, they run the risk of antagonizing the intruders and escalating the intensity of their own next raids.'

One hacker was told that the security of the San Francisco-based United States Leasing's system was too tight. The hacker replied, "No security is too tight.' To prove his point, the hacker entered the system and caused $250,000 worth of damage through sabotage.

One of the classic hacker programs making the rounds of the Massachusetts Institute of Technology was the surreptitiously placed 'Cookie Monster' program. When someone working on a computer least expected it, the screen would suddenly flash the word 'cookie'. If the startled programmer didn't respond, the concealed cookie monster would go berserk, writing 'cookie' over and over, obliterating whatever was on the screen, leaving the final demand: 'Gimme cookie.' The only way to stop the monster was to feed it by typing in the word 'cookie'.

Maxfield discovered that hackers embody the cheerful indifference to conventional morality of their forerunners, the Yippie-inspired 'phone phreaks' of the early 19705. In the hacker's handbook, property rights do not exist, nor does privacy. Imahacker, for instance, posted a message on his BBS: 'If you want to make a prank call to the President of the United States, well, here's the phone number to dial.'

"This was a direct line right to Reagan's desk in the Oval office and, believe me, this was the real number,' says Maxfield. 'He
even told them to use a payphone so that, if you got traced,
you could run.'

With their adventurous amorality, phreakers encountered unexpected risks. Maxfield remembers when phone phreaks in the 196o5 built blue boxes for the Mafia. 'Once they delivered the blue boxes, they were killed so they couldn't rat on their customers to the FBI,' he says. 'So the hackers are dangerous to themselves. They're also a danger to society. They have absolutely no thought for the ultimate consequences of their actions. They're only living in the here and now. They're so immersed in this fictional world inside the computers and networks that they really don't think about the consequences.

They're extremely ego-centred and hacking in itself is extremely addictive because of this constant reinforcement and thrill. It's just like a drug addict who keeps taking stronger and stronger doses of a drug to attain better highs. They keep climbing to greater heights of audacity in their hacking.

'One night,' says Maxfield, 'they tried to connect the Pope with Queen Elizabeth and President Reagan. The Pope was asleep; the Queen's secretary refused the call and Reagan was not in the White House.'

Two of the telephone numbers came from the son of the British diplomat. The diplomat's son posted others on his BBS including the password to the reservation system of the Holiday Inn in Cambodia, the British VD hotline, Dial-an-Atheist, earthquake reports and the British Stock Exchange report.

While the diplomat's son eventually got caught, a hacker named Mad Marvin from Phoenix, Arizona, picked up where he left off. 'Call the embassy of the USSR in Tokyo, Japan,' he wrote on his BBS, as he proceeded to list all of the names of the staff and their direct lines. Scattered among the list were a number of KGB operatives. Right after this message was posted on several boards, the sysop of the World of Cryton BBS and about fifteen other hackers set up a long-distance conference call and dialled the Russian embassy in Tokvo and spent three
attaché and the military and air attaché. 'They were offering hours on the phone talking to the sovache. They were

offering their hacking and phreaking services to the KGB,' said Maxfield.
Luckily I had an informant that was a part of the gang and I was able to report this to the Defense Department.' Soon after he did, Mad Marvin disappeared from the hacker boards.
'It shows you the extent that they'll go to when they're thrill seeking,' says Maxfield. 'What could be more of a thrill than, "Let's call the KGB"? I mean, we're talking sedition and treason but they are kids in a totally unsupervised, unstructured, uncontrolled environment.'

Hacking is perfect for spying, says Maxfield, because it's such a clandestine activity to start with. Hackers camouflage their calls by using 'network weaving', a technique using numerous links that make calls virtually untraceable. Joe, a phone phreak in Texas, leaves a tangled trail behind him whenever he phreaks a call. He has perfect phone pitch and is able to phreak his calls by whistling the numbered tone signals of his blue box. He is so good that he has been able to use the technique to dial direct to Moscow, talking at length to English-speaking disc jockeys on Radio Moscow.

Joe is one of Maxfield's informants, part of his electronic network of spies that have helped him track down criminal hackers in North America, England, Sweden, Denmark, the Netherlands, West Germany, Italy, Argentina, South America, Australia and Japan. But for his work on the celebrated 414 case, Maxfield did not use any informants.

The leader of the 414 gang was a 17-year-old, all-American type, Neal Patrick. He joined a Boy Scout Explorer troop headed by Dennis Bayne, a system-engineering manager at IBM. As Neal and his friends learned more about computers, they began trading information. Soon they decided to form an exclusive computer group. They called themselves the 414 gang because 414 happened to be the three-digit area code for their hometown, Milwaukee, Wisconsin.

'They had a secret bulletin board, recalls Maxfield. In fact, it was so secret, you never saw it advertised. It was strictly an invitation-only type system. I found out about it by intercepting a message on the sting board (the hacking and phreaking section he created for the FBI sting operation). I took a chance and sent a message to the leader of the gang explaining what phreaking tutorial services I could offer members and asking permission for the password to the bulletin board. I pretended that someone «in the know" had actually told me about the secret bulletin board.'

Patrick sent a message to Cable Pair welcoming him as a member of the board. 'From that point on it was all down hill. We began reading all their messages about the computers they were getting into.'

In the beginning, the 414s stumbled across a BBS in New York called oSUNY - Ohio Scientific Users of New York.

The OSUNY BBS was a treasure trove of secret messages and codes posted by users who shared access numbers to MCI and Sprint long-distance telephone services. The users also gave instructions in ways to avoid having unauthorised phone calls traced. The 414 also posted a variety of data network numbers, such as subscribers to Telemail, and added How To' tips for gaining access to major computer systems around the country.

Working independently, and mostly at night, members of the 414 gang accessed computers on GTE's Telenet network.

The way a given computer answered back indicated what sort of machine it was. Since each computer had its own format for permitting access, that narrowed the range of possible passwords.
At times, there was hardly any challenge at all: hackers on the OSUNY or other BBSs to which the 414 gang had access had already posted the passwords. But even guessing them took little effort. Many companies never bothered to change their sample passwords supplied by their computer manufacturer.

By using his father's TRS-So Model II computer and an automatic redial modem, Neal Patrick could break into a system using passwords such as 'system', 'demo' or 'test'.
Patrick pointed out that one of the 414s broke into New York's Sloan-Kettering cancer centre computer by using the name 'test' and the password 'test'. By doing so, they gained privileged-user status by using the help menu and typing 'set process/priv=all'.

When a 414 member used his $1,200 Apple I to gain access to the Sloan-Kettering computer on 3 June 1983, it crashed.

The computer was used to bill other hospitals for computer services and to monitor doses of radiation given to patients at Sloan-Kettering. In all, the 414 gang made some eighty intrusions on the computer.

When the 414s broke into the Los Alamos National Laboratory in New Mexico (where nuclear missiles are made and

tested), they were a heartbeat away from accessing information relating to the design of nuclear weapons. The 414s gained unauthorised access to a data base shared by subcontractors, academics doing research, and employees of Department of Energy contractors. The electronic break in at Los Alamos that led to the detection of the 414 gang took place on 28 June 1983, less than a month after the Sloan-Kettering crash.
At around the same time as the Los Alamos activity, personnel of the Security Pacific Bank in Los Angeles noticed unauthorised access into a computer's system being used by the bank for program development. It was at this time that the bank decided to keep 414 leader, Neal Patrick on the line with a "Super Star Trek' simulator.
It wasn't only the Star Trek simulation that foiled the 414 gang. 'Hackers are creatures of the night,' says Maxfield. 'They have the mistaken idea that it's safer to break in at midnight when no one is around. But if they did it during the day, they would be surrounded by legitimate users and wouldn't be noticed.' In late July 1983, two FBI agents showed up at Neal Patrick's home. Search-warrants were served, based on suspicions that the gang had broken into sixty business and government computer systems in the United States and Canada.

The 414s both delighted and scared people. Their hacking provoked emotive responses from federal officials who wanted to put a stop to an epidemic of computer tampering. Said one shaken-up Pentagon spokesman: 'It's time to put the fear of God into these people.'

Neal Patrick, leader of the 414 gang and a junior at Rufus High School in Milwaukee, became an instant star, appearing on the cover of Newsweek, being interviewed on the phi Donahue television show and guesting on the Today Show.

The media fell in love with the hackers who entered restricted systems. Patrick was invited to testify before a congressional committee studying computer security. Within two months, the first federal computer-crime law was passed.

The capture of the 414 gang marked the beginning of the end for Maxfield. By December 1983, he had worked for eighteen months undercover. While neither the 414s nor the Inner Circle realised who had prompted their demise, Maxfield's days as an FBI informant were numbered.

The Phalse gang specialised in hacking IBM voice-mail systems. IBM had introduced voice mail for their own internal use. Voice mail or Audio Distribution Systems (ADS) enable users with touch-tone phones to send voice messages back and forth to each other. For the Phalse gang it was an irresistible toy. They could eavesdrop on others and use the system to communicate with each other.

Maxfield had followed the gang for several months, tracking them on systems in Paris, Rome, Canada - wherever IBM had a voice-mail network. Because wherever one existed, the Phalse gang had gained control of it through knowing the passwords.

The leader of the Phalse gang, Eric Corley, gave Maxheld's alias, Cable Pair, an account. 'I was a member of the gang; says Maxfield. 'They were using one particular voice-mail system as a super, secret, hidden, private bulletin board and using the system's facilities they had broken into to exchange information about committing further crimes.
Some of these guys were keeping score. "I destroyed five systems last week, how many did you destroy?" They would just chortle every time they ripped somebody off. I got so angry.
There were thousands of these hackers who essentially had a free hand to do anything that they wanted to do and they were doing it.

I had been undercover for almost one and a half years and I was feeling the strain,' recalls Maxfield. 'It was also very frustrating because all these crimes were being committed and the FBI's approach was to gather intelligence. In other words, they were not allowed to tell the victims or warn them. The victims had to come to the FBI. That's the way it was. The FBI is not like a local police department. Their primary mission is intelligence gathering.'

The Phalse gang had penetrated IBM's computer network, taking over forty-six accounts. 'This system was being raped and pillaged and my contact at the Bureau said, "I'm sorry, but we can't do anything about it until they discover it and call us." It was totally frustrating.

'Finally, I just broke ... I wanted to get these guys. They were just destroying the system. They had complete control over it and the victim wasn't even aware of what was going on. They would have found out eventually, but, by that time, there would have been major damage. My idea was prevention, stop them before they get started.'
Maxfield, out of frustration and anger, sent a warning message to the console operator. 'What I didn't know was that the hackers had control over the operator's account. I sent the message on a weekend, which was a mistake. I should have

waited until someone was there. The operator eventually received my warning, but the hackers intercepted it first. I basically said, "Call the FBI." But it came from my account, which had been given to me by the leader of Phalse, so the hackers knew that the warning came from me. In other words,' says Maxfield, 'I broke my cover.'

Immediately following the interception of Maxfield's mes-sage, the leader of the Phase gang called the FBI and successfully impersonated an executive of IBM and said to the FBI agent on the phone, 'What's going on? I got a message saying there's hackers in our computer and I should call you.' The agent, according to Maxfield, did not verify the identity of the person he was speaking with by requesting the telephone number of the caller and ringing him back. In fact, says Maxfield, 'He spilled the whole story of the investigation and my role as an informant to what he thought was the security director of IBM when, in fact, it was the leader of Phalse.' Eric Corley successfully impersonated the IBM ADS systems controller and spoke at great length with the FBI agent, ask-ing, for instance, how informants become members of hacker gangs.

'These people [hackers] are very hungry for technical avenues through which they can communicate,' said the agent. 'You feed them a little bit of bait and a lot of times they'll go for it. You enter into a dialogue with them and they end up taking you for a ride.' Corley tape recorded the conversation he had with the FBI agent and published a verbatim manuscript of it in the first volume of 2600, the monthly magazine for phreakers and hackers.

The agent, not realising he was talking to a hacker, spoke of Maxfield's role as an informant for the FBI: 'We are kind of unique in that we do not have any other source available in any other part of the country that could supply us with information like this.'

On Monday, when IBM's real ADS system controller responded to Maxfield's warning, the agent rang Maxfield.

What's going on? I think we've been had. I just got a call from the ADS controller at IBM.'

Then the agent told him about the first phone call.

"Oh shit,' said Maxfield. 'My cover is blown.'

The agent in charge of the investigation was suspended without pay for thirty days. 'He was sent to FBI purgatory,' says Maxfield.

From the beginning while he was an informant for the FBI, Maxfield sensed that there was 'a concern that I might go native. When the cover was blown, I think there was a feeling that perhaps I had changed sides and it was a deliberate set-up to embarrass the FBI. I think the initial reaction of the FBI was, "that son of a bitch Maxfield set us up."

'I was more concerned at first with the hackers calling in death threats on the phone but also I was waiting for the FBI hit squad to come and wipe me out. ... Paranoia struck.
You're under attack, you're under great stress, your cover's in ruins, you know the FBI is extremely angry at you even though it wasn't totally your fault.'
John Maxfield, from an outsider's point of view, had played both sides against the middle, a deadly consequence of being an over-exposed informant. His story is not far from the realities of spies and agents who make their living by keeping secrets.

Maxfield describes what happened next by literally quoting chapter and verse from the FBI manual: 'Chapter 3, paragraph 19, subsection 5, which deals with informants, says that if your informant's cover is blown, you deny his existence.'

Cable Pair was on his own.

'The hackers knew who I was, because I'd met some of them personally. I had even invited them to come to my office. It was a very frightening time for about the first month or so. I would get threats like they were going to break every bone in my body, they were going to bomb my house, rape my wife, kidnap the kids and poison my dog.

'You see, we had no experience. Nothing to base it on; so i was a very scary time. You know ... are these guys going come around? I mean, I fully expected to have my office fire bombed. I thought somebody was going to accost me in the street; pull out a gun and shoot me. You know, I fully expected that to happen. It never happened ... that's not to say it couldn't still happen.

'They want to put me out of business. I could be murdered by hackers in the next couple of months. As an ex-hacker, I understand. They know I know all of them. I know their identities. I have 7,000 of them logged on my computer. They laugh at the FBI, Secret Service, MCI, Sprint, but they don't laugh at me. I was one of them. I'm a real hacker and they're not. It's a matter of professional jealousy. Most of them have no real technical skill. They're wimps and nerds, but they live in a world in which they are gods.

'I force them to recognise themselves for what they are. I'm the one who rips off their masks. I deliberately go out of my way to draw their fire. I'm gunning for the Glitch so he will slip up and I'll get him. How do you find out where they are without exposing yourself?'

Maxfield was pilloried in the first issue of 2600, and he received plenty of electronic hate mail. According to the hackers, he is a traitor. They do not fear him so much as despise him.
The hackers thought they made a big score by pulling off my mask,' he says. 'To them, it was like pulling off the mask of Darth Vader.'

Within a short period, Maxfield began receiving offers of support from hackers who wanted to change sides and work for him as informants. 'They saw it as an opportunity to get out before it was too late,' he says.

Donn Parker, senior management consultant at SRI, spoke with Maxfield after his cover was blown and encouraged him to continue in private practice. Parker has written five books on the topic of computer crime and is regarded as one of the world's leading authorities on the subject. Parker believes John Maxfield is 'a legend in his own time. I think his work is very valuable. He's probably the most knowledgeable person I know on the subject of hackers. He's gained a great deal of respect from the law-enforcement community and has helped solve many cases.'

"Maxfield,' says Parker, is an enigma. He is simultaneously trusted and regarded with suspicion by the criminal-iustice system, the commercial computer user and hackers. One thing is obvious: he is as fascinated by chasing them as they are addicted to hacking.'

Besides acting as a consultant to a broad spectrum of clients, including banks and government agencies, Maxfield has a lot on his hands these days. The computer hackers are growing up to be computer criminals.

These guys have graduated from War Games to the real underworld,' says Maxfield. For example, there is an orderly exchange of credit-card numbers out there. This is the organised crime of the future. There is virtually no exposure,' noting that a teenager with a Sigo computer, a $so modem and a telephone can sit in his bedroom and rob a bank 2,000 miles away. 'Who needs a gun? And there's no physical evidence. No fingerprints. No trails.

In the United Kingdom, the amount of money defrauded by computer criminals in an average case has risen from €3 1,000 in 1983 to £389,66o in 1988. The maximum single loss recorded among detected cases has also risen during the same period from £500,000 to fro million.
Total annual sterling losses caused by computer crime exceed some to million.? Banks, brokerages and investment firms suffered the most. Of the known cases, 2s per cent did not result in prosecution. Typically, only 15 per cent of all computer crime is reported. In some cases, employers felt the adverse publicity would damage the corporate image or the company's share price.

Estimates of computer fraud vary, but they are considered to be 53-5 billion annually for US businesses alone.$
Compute fraud has obvious appeal. Experts at the FBI say only one out of 22,000 computer criminals is sent to prison. They estimate that only 1 per cent of all computer crime is detected, only 14 per cent of that is reported, and only 3 per cent of those cases ever result in jail sentences. The average dollar amount in reported computer frauds is estimated by the FBI to be $600,000 versus an average of $23,000 using manual methods.to Still, the maximum sentence is one year and a $5,000 fine.

To this day, Maxfield's investigations have resulted in more prosecutions of computer hackers than anyone else in the field.
The biggest computer crime detected by Maxfield involved a hacker who broke into the Bell Telephone Laboratories and stole Sr million of proprietory software. Maxfield's intelligence gathering helped to identify the intruder as Shadow Hawk, a hacker living in Chicago.

As hackers like Shadow Hawk mature, they typically become successful, highly valued employees of corporations. Their career goals will be well-defined and they will continue to respond to technological challenges in an intellectual, clever and personal way. Unless action is taken during the next twenty years, many of the hacker vandals of the early 198os

will continue to manipulate computers and data bases but regard any thefts as 'borrowing', thus avoiding any difficult moral dilemmas.
Today's hackers, unless instilled with a code of ethics, will be tomorrow's computer criminals who will feel no guilt at stealing from huge, impersonal organisations. To their colleagues and superiors, computer criminals will seem completely trust-worthy.

The computer technology they've learned to master at a young age will develop greatly during their lifetime, and, as they mature, so will the power of computers. What we've seen so far has been literally child's play. In the years to come, advanced technology will be in the hands of far more people.

By scanning today's electronic bulletin boards, John Maxfield, in part, is tracking tomorrow's computer felons.

'I had the naive hope that I could stop it before it got started,' says Maxfield. 'But it's always gotten worse. One thing is certain, I'll never lack employment. The hackers will follow me to the ends of the earth to get their revenge and if I retire, it would be a victory for them. You gotta understand,' he says, 'I could walk away from all of this tomorrow and go back to fixing teletype machines and facsimile recorders and installing telephone equipment, but then the hackers would have won. It would be their victory. I really have no choice but to continue.'
The sun has set hours before Maxfield decides it's time to go home. He flicks off his computer terminal and grabs his jacket. As he heads out into the damp Detroit night, Maxfield walks past an autographed picture of James Doohan, the actor who played Scotty in Star Trek. Above Doohan's signature is the command: 'Warp speed, Captain Maxfield'.